IN THE CLAIMS

For the convenience of the Examiner, all pending claims of the present Application are shown below in numerical order whether or not an amendment has been made.

1. (Previously Presented) A method comprising:

intercepting at an agent a first request to grant a web service customer access to a first web service, the agent residing between the web service customer and the first web service and between the web service customer and a second web service;

collecting at the agent one or more authentication credentials of the web service customer;

determining at the agent whether the web service customer is authenticated and authorized;

if the web service customer is authenticated and authorized, at the agent:

granting the first request;

initiating creation of a session and a session ticket;

obtaining a session ticket ID for the session ticket; and

encrypting the session ticket ID and a public key into an assertion;

intercepting at the agent a second request to grant the web service customer access to the second web service, the second request comprising the assertion and a signature associated with a private key; and

if the private key matches the public key in the assertion, granting at the agent the second request without reauthenticating or reauthorizing the web service customer.

2. (Canceled)

3. (Previously Presented) The method of claim 1, wherein the assertion comprises a Security Assertions Markup Language (SAML) assertion.

4. (Canceled)

5. (Previously Presented) The method of claim 1, wherein the agent comprises an Extensible Markup Language (XML) agent.

6. (Original) The method of claim 1, wherein determining whether the web service customer is authenticated and authorized comprises comparing the web service customer with a database containing authentication and authorization data.

7. (Currently Amended) A method comprising:

intercepting at an agent a request to grant a web service customer access to a first web service, the agent residing between the web service customer and the first web service and between the web service customer and a second web service, the request comprising an encrypted assertion and a signature associated with a private key, the encrypted assertion comprising a session ticket ID for a session ticket obtained prior to the request and in response to authentication and authorization of the web service customer for access to the second web service; and

if the private key matches ~~the~~ a public key in the assertion, granting at the agent the ~~second~~ request without reauthenticating or reauthorizing the web service customer.

8. (Previously Presented) The method of claim 7, wherein the assertion comprises a Security Assertions Markup Language (SAML) assertion.

9-23 (Canceled)

24. (Previously Presented) The method of claim 1:

wherein the first request and the second request both originate at the web service customer; and

the method further comprising communicating the assertion to the web service customer to enable the web service customer to access the second web service without reauthentication or reauthorization after the web service customer accesses the first web service.

25. (Previously Presented) The method of claim 1:

wherein the first request originates at the web service customer and the second request originates at the first web service; and

the method further comprising communicating the assertion to the first web service to enable the web service customer to access the second web service without reauthentication or reauthorization after the web service customer accesses the first web service.

26. (Currently Amended) An apparatus comprising:

one or more processors residing between a ~~the~~ web service customer and a ~~the~~ first web service and between the web service customer and a ~~the~~ second web service; and

a memory coupled to the processors comprising one or more instructions executable at the processors, the processors operable when executing the instructions to:

intercept a first request to grant ~~a~~ the web service customer access to ~~a~~ the first web service;

collect one or more authentication credentials of the web service customer;

determine whether the web service customer is authenticated and authorized;

if the web service customer is authenticated and authorized:

grant the first request;

initiate creation of a session and a session ticket;

obtain a session ticket ID for the session ticket ; and

encrypt the session ticket ID and a public key into an assertion;

intercept a second request to grant the web service customer access to the second web service, the second request comprising the assertion and a signature associated with a private key; and

if the private key matches the public key in the assertion, grant the second request without reauthenticating or reauthorizing the web service customer.

27. (Previously Presented) The apparatus of claim 26, wherein the assertion comprises a Security Assertions Markup Language (SAML) assertion.

28. (Previously Presented) The apparatus of claim 26, wherein the agent comprises an Extensible Markup Language (XML) agent.

29. (Previously Presented) The apparatus of claim 26, wherein the processors are further operable when executing the instructions to determine whether the web service customer is authenticated and authorized by comparing the web service customer with a database containing authentication and authorization data.

30. (Currently Amended) The apparatus of claim 26, wherein:

the first request and the second request both originate at the web service customer; and

the processors are further operable when executing the instructions to communicate ~~communicating~~ the assertion to the web service customer to enable the web service customer to access the second web service without reauthentication or reauthorization after the web service customer accesses the first web service.

31. (Previously Presented) The apparatus of claim 26, wherein:

the first request originates at the web service customer and the second request originates at the first web service; and

the processors are further operable when executing the instructions to communicate the assertion to the first web service to enable the web service customer to access the second web service without reauthentication or reauthorization after the web service customer accesses the first web service.

32. (Currently Amended) A system comprising:

a first web service;

a second web service; and

an agent residing between a web service customer and the first web service and between the web service customer and the second web service, the agent residing on a processor-controlled server and operable to:

intercept a first request to grant the web service customer access to the first web service;

collect one or more authentication credentials of the web service customer;

determine whether the web service customer is authenticated and authorized, and if the web service customer is authenticated and authorized:

grant the first request;

initiate creation of a session and a session ticket;

obtain a session ticket ID for the session ticket; and

encrypt the session ticket ID and a public key into an assertion;

intercept a second request to grant the web service customer access to the second web service, the second request comprising the assertion and a signature associated with a private key; and

if the private key matches the public key in the assertion, grant the second request without reauthenticating or reauthorizing the web service customer.

33. (Previously Presented) The method of Claim 1, further comprising

at the agent, placing the assertion into a header;

sending the assertion to the first web service;

returning the assertion to the web service consumer.

34. (Previously Presented) The method of Claim 1, wherein the second request comprises an XML document containing the assertion; and

wherein the web service customer has signed the XML document with the private key.

35. (Previously Presented) The method of Claim 1, wherein granting at the agent the second request without reauthenticating or reauthorizing the web service customer further comprises:

using, at the agent, the session ticket ID with the assertion to determine if the web service customer is authenticated to access the second web service; and

if the user is authenticated, granting at the agent the second request without reauthenticating or reauthorizing the web service customer.

36. (Previously Presented) The method of Claim 1, wherein the second request is intercepted at the agent before reaching the second web service.

37. (Previously Presented) The method of Claim 25, wherein the second request is intercepted at the agent before reaching the second web service.

38. (Previously Presented) The method of Claim 1, further comprising determining at the agent whether the public key matches the private key.

39. (Previously Presented) The method of Claim 25, wherein the second request originates at the first web service independent of the web service customer requesting access to the second web service.

40. (New) The method of claim 7, wherein the request originates at the web service customer.

41. (New) The method of claim 7, wherein request originates at the second web service.